OLLSCOIL NA hÉIREANN, GAILLIMH

NATIONAL UNIVERSITY OF IRELAND, GALWAY

AUTUMN EXAMINATIONS 2008 – HONOURS

B.A. and B.Sc EXAMINATIONS

MATHEMATICS

MA416 [RING THEORY] and MA491 [FIELD THEORY]

Professor D. Armitage
Professor J. Hinde
Professor T. Hurley
Dr R. Quinlan
Dr J. Ward

Those seeking credit for one semester should answer *three* questions.
Those seeking credit for both semesters should answer *five* questions.
Please use separate answer books for each section.

Time Allowed : **Three** hours

Section A – Ring Theory (MA416)

A1. (a) Give an example of

i. A ring;
ii. A non-commutative ring;
iii. A non-commutative ring having an uncountable number of elements;
iv. A commutative ring having a finite number of elements;
v. A non-commutative ring with exactly 8 elements.

(b) What is meant by a *zero-divisor* in a communtative ring R with identity?
Suppose that both a and b are zero-divisors in R. Must it follow that the sum $a+b$ is also a zero-divisor?
What are the zero-divisors in the ring $D_3(\mathbb{Q})$ of diagonal 3×3 matrices with rational entries?

(c) Let R be a commutative ring with an identity element for multiplication. What is meant by a *unit* in R?
Prove that the product of two units in R is again a unit. What are the units of the ring $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries?

(d) Suppose that R is a ring and that a and b are elements of R having the property that the product ab is the zero element of R. Must it be the case that the product ba is also the zero element of R?

P.T.O.

A2. (a) Let F be a field. What is meant by an *irreducible* polynomial in the ring $F[x]$ of polynomials with coefficients in F?
State the division algorithm for polynomials in $F[x]$.
Hence or otherwise show that if a polynomial $f(x)$ of degree at least 2 in $F[x]$ has a root in F, then $f(x)$ is reducible in $F[x]$.

(b) What is meant by a *primitive* polynomial in $\mathbb{Z}[x]$? Show that the product of two primitive polynomials is again primitive.
Suppose that $f(x)$ and $g(x)$ are (non-constant) polynomials in $\mathbb{Z}[x]$ with the property that the product $f(x)g(x)$ is primitive. Does it follow that $f(x)$ and $g(x)$ are both primitive?

(c) Give an example (with explanation) of

i. A polynomial in $\mathbb{Q}[x]$ that has no root in $\mathbb{Q}$ but is reducible in $\mathbb{Q}[x]$.

ii. An polynomial of degree at least 2 that has rational coefficients and is irreducible in $\mathbb{R}[x]$.

iii. An irreducible polynomial of degree 5 in $\mathbb{Z}[x]$.

iv. An irreducible polynomial of degree 3 in $\mathbb{F}_2[x]$ (here $\mathbb{F}_2$ denotes the field $\mathbb{Z}/2\mathbb{Z}$ of two elements).

(d) For each of the following polynomials, determine, with explanation, if it is irreducible in the indicated ring.

i. $4x^6 - 3x^5 + 6x^3 - 12x^2 + 9x - 15$, in $\mathbb{Q}[x]$

ii. $x^4 - 7x^3 + 10x^2 + 8x - 6$, in $\mathbb{Z}[x]$

iii. $2x^3 + 2x^2 + 1$, in $\mathbb{F}_3[x]$ (here $\mathbb{F}_3$ denotes the field $\mathbb{Z}/3\mathbb{Z}$ of integers modulo 3).

iv. $3x^2 - 4x + 6$, in $\mathbb{R}[x]$.

A3. (a) Let R and S be rings.What is meant by a *ring homomorphism* $\phi : R \longrightarrow S$?
Two functions $\phi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}$ and $\psi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}$ are defined as follows for $f(x) \in \mathbb{Q}[x]$.

- $\phi(f(x))$ is defined to be the *leading* coefficient of $f(x)$, for $f(x) \neq 0$. ($\phi(f(x)) = 0$ if $f(x)$ is the zero polynomial).
- $\psi(f(x))$ is defined to be the constant coefficient of $f(x)$.

Determine, with explanation, whether each of the functions ϕ and ψ is a ring homomorphism.

(b) What is meant by a (two-sided) *ideal* of a ring R?
If $\phi : R \longrightarrow S$ is a ring homomorphism, define the *kernel* of ϕ and prove that it is a two-sided ideal of R.

(c) What is meant by a *principal ideal* in a commutative ring with identity?
Give an example, with explanation, of a commutative ring with identity that contains non-principal ideals.
What is meant by a *principal ideal domain (PID)*?
Prove that the ring of integers $\mathbb{Z}$ is a PID.

P.T.O.

A4. (a) What is meant by a *maximal ideal* in a commutative ring with identity?
What is meant by a *prime ideal* in a commutative ring with identity?
Give an example (with explanation) of

i. A prime ideal of $\mathbb{Q}[x]$.
ii. An ideal of $\mathbb{Q}[x]$ that is not prime.
iii. A (non-zero) ideal that is prime but not maximal, in some commutative ring with identity.

(b) What is meant by an *irreducible element* in a commutative ring with identity?
What is meant by a *prime element* in a commutative ring with identity?
Prove that in a commutative ring with identity, every prime element is irreducible.

(c) Let R denote the ring consisting of those complex numbers of the form $a + b\sqrt{-5}$, where a and b are integers, under the usual addition and multiplication of complex numbers. Show that R contains irreducible elements that are not prime.

Section B – Field Theory (MA 491)

B1. (a) Explain how a field $\mathbb{K}$ may be viewed as a vector space over a sub–field $\mathbb{F}$ and hence define the **degree** $[\mathbb{K} : \mathbb{F}]$.
(b) Define the term **splitting field** of a polynomial. Find quadratic factors for the polynomial

$$f(x) = x^4 + 2x^3 - 8x^2 - 6x - 1$$

over $\mathbb{Z}[x]$ and hence, or otherwise show that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field for $f(x)$ over $\mathbb{Q}$.
(c) Show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ and deduce that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is an extension of degree 4 over $\mathbb{Q}$. Write down a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.
(d) Prove that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{3} - \sqrt{2})$, and find the minimum polynomial of $\sqrt{3} - \sqrt{2}$ over $\mathbb{Q}(\sqrt{3})$.

B2. (a) What is meant by a "straight–edge and compass construction"?
(b) State Gauss' Theorem concerning the values for which the regular n–gon can be constructed by straight edge and compass.
(c) Using part (ii) show that 18° **is** constructible. Deduce that the angle n° is constructible $\Leftrightarrow 3|n$.
(d) State a necessary condition for an algebraic number α to be constructible using straight–edge and compass. Hence **prove** that the regular heptagon is not constructible using straight–edge and compass.
(e) Show that $\cos^{-1}\left(\dfrac{11}{16}\right)$ can be trisected using straight–edge and compass.

B3. (a) Write down the four roots of the polynomial $x^4 - 2$. Letting $r = \sqrt[4]{2}$ and $i = \sqrt{-1}$, show that a splitting field for this polynomial over $\mathbb{Q}$ is $\mathbb{Q}(r, i)$.
(b) Let σ be the $\mathbb{Q}$–automorphism defined as $\sigma : r \mapsto ir; \quad \sigma : i \mapsto i$, and let τ be the $\mathbb{Q}$–automorphism of complex conjugation, i. e. $\tau : i \mapsto -i; \quad \tau : r \mapsto r$. Hence determine the Galois group G of $x^4 - 2$ over $\mathbb{Q}$ and establish that G is non–abelian of order 8.
(c) Under the Galois correspondence find the (fixed) subfield corresponding to the subgroup of G of order 2 generated by σ^2.

P. T. O.

B4. (a) Let $\mathbb{F}_q$ be a finite field of order q $(= p^n,\ p$ a prime $n \geq 1)$. State the main properties of $\mathbb{F}_q$.

(b) Prove Gauss' formula

$$N_q(d) = \frac{1}{d} \sum_{k|d} \mu\left(\frac{d}{k}\right) q^k$$

where $N_q(d)$ is the number of monic irreducible polynomials of degree d over the finite field of order q.

(c) By factorising $x^{16} - x$ over the field of two elements $\mathbb{F}_2$, or otherwise, determine the irreducible polynomials of degree 4 over the field of two elements $\mathbb{F}_2$.

(d) Choosing any of the irreducible quartics in part (c), show that it can be factored into a product of two irreducible quadratics over $\mathbb{F}_4$, the finite field of order 4.